Amendments to the Specification:

Please replace the title as follows:

~~METHOD FOR AUTOMATED GENERATION OF ACCESS CONTROLLED,~~

~~PERSONALIZED DATA AND/OR PROGRAMS~~

METHOD OF AUTOMATED GENERATION OF ACCESS-CONTROLLED,

PERSONALIZED DATA AND/OR PROGRAMS

Please replace the paragraph beginning on page 2, line 17 (as amended in the Annexes to the International Preliminary Report on Patentability), with the following rewritten paragraph:

Described in the publication US 2003/0084184 is a communication system for monitoring and control of communication time and/or communication costs, the user being informed about the used and/or still remaining communication time, and communication being interrupted after the limit value has been reached. Communication between the client and the host system is established via a Virtual Session Manager (VSM). The quantity of information exchanged between the mobile client and the host system is decreased considerably, whereby costs for the user are reduced. However this document also does not disclose any user-specific generation of data and/or programs.

Please replace the paragraph beginning on page 7, line 23, with the following rewritten paragraph:

The user 10,...,14 is identified by the central unit 40, an authorization class being assigned to the user 10,...,14 by means of a user database 45. Personal identification numbers (PIN) and/or so-called smart cards can be used for identification, for instance. Smart cards normally presuppose a card reader at the communication device 20,...,24. In both cases the name or another identification of the user 10,...,14 as well as the PIN are transmitted to the central unit 40 or to a trusted remote server. An identification module 44 or respectively authentication module 44 decrypts (if necessary) and checks the PIN via the user database 45. As an embodiment variation, credit cards can also be used for identification of the user 10,...,14. If the user 10,...,14 uses his credit card, he can likewise enter his PIN. The magnetic strip of the credit card typically contains the account number and the encrypted PIN of the authorized owner, i.e. in this case of the user 10,...,14. The decryption can take place directly in the card reader itself, as is common in the state of the art. Smart cards have the advantage that they make possible greater security against fraud through an additional encryption of the PIN. This encryption can take place either through a dynamic coding scheme containing e.g. time, day or month, or another algorithm. The decryption and identification does not take place in the apparatus itself, but externally via the identification module 45. A further possibility is a chipcard inserted directly into the communication device 20,...,24. The chipcard can be, for instance, an SIM card (Subscriber Identification Module) or smart card, a call number being assigned to the chipcards in each case. The assignment can be carried out, for example, via an HLR (Home Location Register), by the IMSI (International Mobile Subscriber Identification), e.g. an MSISDN (Mobile Subscriber ISDN), being stored assigned to a call number in the ~~HRL~~HLR. An unambiguous identification of the user 10,...,14 is possible then via this assignment.

Please replace the paragraph beginning on page 8, line 16, with the following rewritten paragraph:

The user 10,...,14 transmits access request data for access to the logical records 421,...,423 of the at least one source database 42 of the communication device 20,...,24 via the network 30/31 to the central unit 40. The access request data can be entered via input elements of the communication device 20,...,24. The input elements may comprise e.g. keyboards, graphic input elements (mouse, trackball, eye tracker with virtual retinal display (VRD), etc.), but also IVR (Interactive Voice Response) etc. The user 10,...,14 has the possibility of determining by himself at least part of the access request data e.g. on the basis of transmitted content indications of the at least one source database 42 and/or access conditions data. This can take place e.g. in that the user is asked by the receiving device 20,...,24 to give his consent via an interface to access conditions or to part of the access conditions. Conditions of access to the data of the source database 42 can include in particular an additional authentication and/or fees for the access. The access request data are checked in the central unit 40, and the desired personalized, access-controlled data and/or programs are then generated on the basis of the authorization class of the user 10,...,14 and the access request data by means of a filter module 41. The personalized data can be generated and transmitted e.g. in HTML (Hyper Text Markup Language) and/or HDML (Handheld Device Markup Language) and/or WML (Wireless Markup Language) and/or VRML (Virtual Reality Modeling Language) and/or ~~ASD~~ ASP (Active Server Pages). This can be carried out e.g. by means of a corresponding module, achieved through hardware and/or software, of the central unit 40. The advantage of the active server technology is, among other things, that it allows a dynamic access interface and/or access surface to be generated for so-called access on demand. Other technologies with similar advantages are also just as conceivable of course.

Please replace the Abstract with the attached amended Abstract.